

1 Teoremas de Sylow

O Teorema de Lagrange (Teorema 1, Notas de aula 1), diz que a ordem de cada subgrupo H de um dado grupo G divide a ordem do próprio G . Uma pergunta natural que surge desse teorema é a seguinte: dado um número n que divide a ordem de um grupo G quando existe um subgrupo de G de ordem n ? Responder essa questão é o objetivo dessa seção.

Antes de concentrarmos esforços nos Teoremas de Sylow, que são a peça chave para responder a essa pergunta, discutiremos ações de grupos em conjunto, um assunto que é de fundamental importância tanto na teoria de grupos, como em aplicações em outras áreas da matemática e até mesmo na física.

Definição 1. Sejam G um grupo e X um conjunto. Uma **ação de G em X** , é uma função $\varphi : G \times X \rightarrow X$, definida por $\varphi(g, x) = gx$, com $g \in G$ e $x \in X$, satisfazendo as seguintes condições:

1. $\varphi(e, x) = x$, para todo $x \in X$;
2. $\varphi(g, \varphi(h, x)) = \varphi(gh, x)$, para quaisquer $g, h \in G$ e $x \in X$.

Notação: $G \curvearrowright X$.

Observação. Por simplicidade utilizaremos a imagem gx para indicar $\varphi(g, x)$.

Exemplo 1. Sejam $X_n = \{1, 2, \dots, n\}$ e $G = S_n$. Considere a função $\psi : G \times X_n \rightarrow X_n$, dada por $\psi(\sigma, i) = \sigma(i)$. É fácil ver que ψ é uma ação de S_n em X_n .

Exemplo 2. Sejam $G = \text{GL}(n, \mathbb{R})$, e $X = \mathbb{R}^n$ o espaço euclidiano n -dimensional. A função $\psi : \text{GL}(n, \mathbb{R}) \times V \rightarrow V$ $\psi(g, v) = g.v$, onde $.$ denota o produto convencional de matrizes, define uma ação de $\text{GL}(n, \mathbb{R})$ em V .

Exemplo 3. Considere $G = \text{O}(n, \mathbb{R})$, e a esfera n -dimensional em $\mathbb{R}^n$, dada por $S^n := \{v \in \mathbb{R}^n; ||v|| = 1\}$. A função $\psi : \text{O}(n, \mathbb{R}) \times S^n \rightarrow S^n$ $\psi(g, v) = g.v$, onde $.$ denota o produto convencional de matrizes, e v é um vetor coluna, define uma ação de $\text{O}(n, \mathbb{R})$ em $\mathbb{R}^n$.

Exemplo 4. Sejam G um grupo e P um subgrupo de G . A função

$$\begin{aligned}\varphi : P \times G &\rightarrow G \\ (p, g) &\mapsto p g p^{-1},\end{aligned}$$

é uma ação, conhecida como **ação por conjugação**.

O próximo exemplo de ação é muito simples, mas nos leva a uma bonita prova do teorema de Cayley.

Exemplo 5. Seja G um grupo, X o conjunto que consiste dos elementos de G , isto é, $X = G$. A função $E : G \times X \rightarrow X$, dada por $E(g, x) = g \cdot x$, onde $\cdot$ denota a operação do grupo é uma ação conhecida como **ação por multiplicação a esquerda**.

Temos o seguinte lema.

Lema 1. *Seja G um grupo, e considere a ação de multiplicação a esquerda por em G . Então $\psi : G \rightarrow S_G$, tal que $\psi(g) = E(g, -)$ é um homomorfismo de grupos.*

Demonstração. Primeiro vamos ver que $\psi : G \rightarrow S_G$ está bem definida, isto é, $\psi(g)$ é um elemento de S_G , ou seja, uma bijeção de G .

Passo 1: Injetividade Fixado $g \in G$, e dados $x, y \in G$ temos que $E(g, x) = E(g, y)$ se, e somente se $gx = gy$, mas como G é grupo, temos que $x = y$. Logo $E(g, -)$ é injetiva.

Passo 2: Sobrejetividade Para qualquer $z \in G$, basta tomar $x = g^{-1}z \in G$ para ver que $E(g, x) = z$. Assim $E(g, -)$ é sobrejetiva e portanto uma bijeção. Logo ψ está bem definida.

Vamos agora provar que $\psi(gh) = E(g, -) \circ E(h, -)$, para quaisquer $g, h \in G$.

De fato, como $\psi(gh) = E(gh, -)$. Temos que $E(gh, x) = (gh)x = g(hx) = gE(h, x) = E(g, E(h, x)) = (E(g, -) \circ E(h, -))(x)$ para todo $x \in G$, assim $\psi(gh) = (E(g, -) \circ E(h, -)) = \psi(g)\psi(h)$ e portanto ψ é homomorfismo. $\square$

Temos agora todos os ingredientes que precisamos para demonstrar o teorema de Cayley.

Teorema 1 (Cayley). *Seja G um grupo de ordem n . Então G é isomorfo a um subgrupo de S_n .*

Demonstração. Considere $\psi : G \rightarrow S_G$ definida no Lema 1. Vamos provar que ψ é injetiva, assim G será isomorfo a $\psi(G)$ pelo Teorema do isomorfismo. Vamos provar que $\ker \psi = e_G$. De fato, seja $x \in \ker \psi$, isto é, $E(x, -) = Id_{S_n}$. Assim, por um lado $E(x, e_G) = x.e = x$, e por outro $E(x, e) = Id_{S_n}(e) = e$. Logo $x = e$ e temos nosso resultado. $\square$

Definição 2. Temos os seguintes subconjuntos “notáveis” de X e G .

1. Dado $x \in X$ definimos como **órbita de x** , e denotaremos por $\mathcal{O}(x)$, o seguinte subconjunto de X :

$$\mathcal{O}(x) := \{gx \in X ; \forall g \in G\}.$$

2. Dado $x \in X$ definimos como **estabilizador de x** , e denotaremos por $\text{Stab}(x)$, o seguinte subconjunto de G :

$$\text{Stab}(x) := \{g \in G ; gx = x; \forall x \in X\}.$$

3. Dizemos que $x \in X$ é um **ponto fixo** da ação se $gx = x$, para todo $g \in G$, ou seja $\text{Stab}(x) = G$.

Denotamos por X^G o conjunto de todos os pontos fixos da ação.

Exemplo 6. Na ação de $\text{GL}(n, \mathbb{R}) \curvearrowright \mathbb{R}^n$, definida no Exemplo 2, se $v \neq 0$, vemos que $\mathcal{O}(v) = \mathbb{R}^n$.

Definição 3. Sejam G um grupo, X um conjunto e $G \curvearrowright X$ uma ação. Se existe $x \in X$ tal que $\mathcal{O}(x) = X$, dizemos que a ação é transitiva.

A ação do Exemplo 6 é transitiva.

Exemplo 7. No exemplo 4 temos que se $g \in G$, então

$$\mathcal{O}(g) = \{pgp^{-1} \in G ; p \in P\}$$

e

$$\text{Stab}(g) = \{p \in P ; pgp^{-1} = g\}.$$

A seguinte proposição é imediata.

Proposição 1. *Seja $G \curvearrowright X$ uma ação. Para todo $x \in X$ temos $\text{Stab}(x) \leq G$.*

O seguinte resultado será usado várias vezes nessa sessão.

Teorema 2 (Órbita-estabilizador). *Seja $G \curvearrowright X$ uma ação. Para todo $x \in X$ a cardinalidade da órbita de x é igual ao índice do estabilizador de x em G , ou seja, $|\mathcal{O}(x)| = |G : \text{Stab}(x)|$.*

Demonstração. Vamos construir uma função bijetiva entre $\mathcal{O}(x) := \{gx; \forall g \in G\}$ e o conjunto das classes laterais de $\text{Stab}(x)$ em G que denotaremos por $G/\text{Stab}(x)$ (CUIDADO!! $G/\text{Stab}(x)$ não é grupo, pois $\text{Stab}(x)$ pode não ser normal, estamos usando aqui apenas a estrutura de conjunto).

Defina $\varphi : \mathcal{O}(x) \rightarrow G/\text{Stab}(x)$ como $\varphi(gx) = g\text{Stab}(x)$.

Afirmção 1: φ está bem definida. De fato, sejam gx e hx dois elementos em $\mathcal{O}(x)$, tais que $gx = hx$, assim $h^{-1}gx = h^{-1}hx = x$. temos que $h^{-1}g \in \text{Stab}(x)$ e portanto $g\text{Stab}(x) = h\text{Stab}(x)$. Logo φ está bem definida.

Afirmção 2: φ é injetiva. De fato, sejam gx e hx dois elementos em $\mathcal{O}(x)$, tais que $\varphi(gx) = \varphi(hx)$, temos que $g\text{Stab}(x) = h\text{Stab}(x)$, mas isso implica que $h^{-1}g \in \text{Stab}(x)$. Por definição então, temos que $h^{-1}gx = x$, e assim $gx = hx$.

Afirmção 3: φ é sobrejetiva. De fato, dado uma classe lateral $g\text{Stab}(x)$, temos que $\varphi(gx) = g\text{Stab}(x)$.

Assim temos que existe uma bijeção entre $\mathcal{O}(x)$ e $G/\text{Stab}(x)$ e portanto eles têm a mesma cardinalidade. Em particular, a cardinalidade de $G/\text{Stab}(x)$ é dada por $(G : \text{Stab}(x))$, de onde segue o resultado. $\square$

Sejam G um grupo, X um conjunto e $G \curvearrowright X$ uma ação. Não é difícil ver que $x \simeq_G y$ se, e somente se, existe $g \in G$, tal que $gx = y$, define em X uma

relação de equivalência. Assim, duas órbitas coincidem, ou são disjuntas. Isso implica que X pode ser escrito como união disjunta das órbitas da ação por G . Isto é $X = \bigcup_{i \in I} \mathcal{O}(x_i)$. Usando essa discussão podemos provar o seguinte lema.

Lema 2. *Seja $G \curvearrowright X$ uma ação, com $|X| < \infty$ e $|G| = p^n$. Então $|X| \equiv |X^G| \pmod{p}$.*

Demonstração. Como X é finito, existem $x_1, \dots, x_k$ tais que podemos escrever $X = \bigcup_{i=1}^k \mathcal{O}(x_i)$, ou ainda $X = X^G \cup \bigcup_i \mathcal{O}(x_i)$ com $|\mathcal{O}(x_i)| > 1$. Logo

$$|X| = |X^G| + \sum |\mathcal{O}(x_i)|, \quad (1)$$

Do teorema da órbita-estabilizador, temos que $|\mathcal{O}(x_i)| = (G : \text{Stab}(x_i))$, e como $(G : \text{Stab}(x_i))$ divide $|G|$ temos que $|\mathcal{O}(x_i)|$ divide a ordem de G . Assim, cada um dos $|\mathcal{O}(x_i)|$ divide p^n , e portanto é divisível por p . Da equação 1, temos o resultado. $\square$

Veremos como usar esses resultados para o estudo de grupos finitos. Seja G um grupo finito e considere o conjunto (subgrupo!) $Cl(g) := \{hgh^{-1}; \forall h \in G\}$. Diremos que os elementos de $Cl(g)$ são os conjugados de g em G . É evidente que $Cl(g) = g$ se, e somente se, $gh = hg$ para todo $h \in G$, isto é $g \in Z(G)$. Considerando a ação de G em G pela conjugação (veja o Exemplo 3), pela discussão do parágrafo anterior, temos que existem $g_1, \dots, g_k$ elementos de G representantes das órbitas, tais que

$$G = \bigcup_{i=1}^k Cl(g_i)$$

Usando a equação acima temos o seguinte conveniente resultado:

Teorema 3 (Equação de Classe). *Seja G um grupo finito. Então*

$$|G| = |Z(G)| + \sum |Cl(g_i)|,$$

com cada $|Cl(g_i)| > 1$.

Antes de discutirmos os Teoremas de Sylow, apresentaremos o importante Teorema de Cauchy.

Teorema 4 (Cauchy). *Sejam G um grupo finito e p um número primo tal que p divide $|G|$. Então G admite um subgrupo de ordem p .*

Demonstração. Sejam $|G| = n$ e $S := \{(a_1, \dots, a_p) \in G^p \mid a_1 a_2 \cdots a_p = e_G\}$. Note que $\#S = n^{p-1}$, de fato, podemos sem perda de generalidade escolher arbitrariamente os $p - 1$ primeiros elementos de S , segue então que $a_p = (a_1 \dots a_{p-1})^{-1}$.

Agora observe que se $s = (a_1, \dots, a_p) \in S$, e σ é a função dada por $\sigma(s) = (a_2, \dots, a_p, a_1)$, então $\sigma(s) \in S$, uma vez que

$$a_1 \cdots a_p = e_G \Rightarrow a_2 \cdots a_p a_1 = e_G.$$

Assim σ é uma permutação de S .

Temos então a ação $\mathbb{Z}_p \curvearrowright S$ dada por

$$\begin{aligned} \psi : \mathbb{Z}_p \times S &\rightarrow S \\ (\bar{r}, s) &\mapsto \sigma^r(s). \end{aligned}$$

Agora, para todo $s \in S$, temos pelo Teorema da órbita-estabilizador que $|\mathcal{O}(s)| = |\mathbb{Z}_p : \text{Stab}(s)|$. Deste modo, como $|\mathbb{Z}_p : \text{Stab}(s)|$ divide $|\mathbb{Z}_p| = p$ pelo Teorema de Lagrange, segue que $|\mathbb{Z}_p : \text{Stab}(s)| = 1$ ou $|\mathbb{Z}_p : \text{Stab}(s)| = p$ para todo $s \in S$.

Note que $|\mathcal{O}(e_G, \dots, e_G)| = 1$. Então $S \setminus \{(e_G, \dots, e_G)\}$ possui $n^{p-1} - 1$ elementos, que estão distribuídos em órbitas de tamanho p ou 1. Logo, existe pelo menos um elemento $s = (a_1, \dots, a_p) \in S \setminus \{(e_G, \dots, e_G)\}$ tal que $|\mathcal{O}(s)| = 1$, pois caso contrário, $S \setminus \{(e_G, \dots, e_G)\}$ estaria dividido em órbitas de tamanho p , ou seja $p/n^{p-1} - 1$, o que é absurdo, já que p/n^{p-1} .

Afirmção: $s = (g, g, \dots, g)$, para algum $g \in G$.

De fato, seja $s = (a_1, \dots, a_p) \in S$, temos que

$$\psi(\bar{0}, s) = \sigma^0(s) = Id(s) = s.$$

Como $|\mathcal{O}(s)| = 1$, segue que $\psi(\bar{i}, s) = \sigma^i(s) = s$ para todo i , ou seja,

$$\begin{aligned} (a_1, \dots, a_p) &= \sigma(s) = (a_2, \dots, a_p, a_1) \\ &= \sigma^2(s) = (a_3, \dots, a_p, a_1, a_2) \\ &\vdots \\ &= \sigma^{p-1}(s) = (a_p, a_1, \dots, a_{p-1}). \end{aligned}$$

Portanto, $a_1 = a_2 = \dots = a_p$ e segue a afirmação.

Pela afirmação, temos $s = (g, \dots, g) \in S$ segue que $g^p = e_G$. E portanto, $\langle g \rangle \leq G$ é o subgrupo desejado. $\square$

Passaremos agora a discutir os subgrupos de Sylow de um dado grupo.

Definição 4. Sejam G um grupo finito e $H \leq G$. Dizemos que H é **p-subgrupo** de G se $|H| = p^n$, para algum n . E dizemos que H é um **p-subgrupo de Sylow** de G se $|H| = p^n$, para algum n e p^n é a maior potência de p que divide a ordem de G .

Se $|G| = 36$, um 2-subgrupo de G , caso exista, tem ordem 2 ou 4, enquanto um 2-subgrupo de Sylow de G , caso exista, tem ordem 4. O próximo teorema garante a existência de tais subgrupos.

Teorema 5 (1º Teorema de Sylow). *Se p é um primo e G é um grupo tal que $|G| = p^r m$ e $p \nmid m$, então para cada inteiro t , $0 \leq t \leq r$, existe um subgrupo H de G tal que $|H| = p^t$.*

Demonstração. Sejam G , p e m como nas hipóteses. Provaremos o teorema de forma indutiva.

Suponha que exista H_i um p -grupo, tal que $|H_i| = p^i$ e $0 \leq i < r$. Considere a ação de $H_i \curvearrowright G/H_i$, dada por

$$\begin{aligned} \psi : H_i \times G/H_i &\rightarrow G/H_i \\ (h, gH_i) &\mapsto hgH_i. \end{aligned}$$

Assim, pelo Lema 2 temos

$$|G/H_i| \equiv |(G/H_i)^{H_i}| \pmod{p}. \quad (2)$$

Temos as seguintes equivalências:

$$\begin{aligned} gH_i \in (G/H_i)^{H_i} &\Leftrightarrow hgH_i = gH_i \quad \forall h \in H_i \\ &\Leftrightarrow g^{-1}hg \in H_i \quad \forall h \in H_i \\ &\Leftrightarrow g^{-1}H_i g \subset H_i \\ &\Leftrightarrow g \in N(H_i) \quad \text{o normalizador de } G. \end{aligned}$$

Portanto, $(G/H_i)^{H_i} = \{gH_i \in G/H_i \mid g \in N(H_i)\} = N(H_i)/H_i$ e como $H_i \triangleleft N(H_i)$, segue que $N(H_i)/H_i$ é grupo. Assim, pela equação (2), temos

$$[G : H_i] \equiv [N(H_i) : H_i] \pmod{p}.$$

Como $|G| = p^r m$ e $|H_i| = p^i$ com $i < r$ segue que p divide $[G : H_i]$ e então p divide $[N(H_i) : H_i]$.

Assim, pelo Teorema de Cauchy, $N(H_i)/H_i$ admite um subgrupo $H_{i+1}/H_i < N(H_i)/H_i$, de ordem p , onde H_{i+1} subgrupo de G . Deste modo, $|H_{i+1}/H_i| = [H_{i+1} : H_i]$ e pelo Teorema de Lagrange, temos

$$|H_{i+1}| = [H_{i+1} : H_i] \cdot |H_i| = p^{i+1}$$

Assim, começando com $H_0 = e_G$, obtemos uma cadeia de grupos

$$H_0 \subset H_1 \subset H_2 \subset \cdots \subset H_r$$

onde cada subgrupo H_i possui ordem p^i para $0 \leq i \leq r$. □

Observe que se p é um primo tal que $p \nmid |G|$, então $\{e\}$ é o único p -subgrupo de Sylow de G .

Teorema 6 (2° Teorema de Sylow). *Se p é um primo e G é um grupo tal que $|G| = p^r m$, $p \nmid m$ e $r \geq 1$. Se H e K são dois p -subgrupos de Sylow de G , então H e K são conjugados, ou seja, $H = gKg^{-1}$ para algum $g \in G$.*

Demonstração. Sejam H, K p -subgrupos de Sylow de G . Considere a ação de $H \curvearrowright G/K$ dada por

$$\begin{aligned}\psi : H \times G/K &\rightarrow G/K \\ (h, gK) &\mapsto hgK.\end{aligned}$$

Assim, temos

$$|G/K| = |(G/K)^H| \pmod{p}. \quad (3)$$

Como $|G/K| = [G : K] \neq 0$, uma vez que K é p -subgrupo de Sylow e portanto próprio. Temos que existe $P \in (G/K)^H$, isto é, a ação de H em G/K admite pelo menos um ponto fixo, que denotaremos por gK .

Segue pela definição de ponto fixo, $hgK = gK$ para todo $h \in H$, ou seja, $g^{-1}hg \in K$ para todo $h \in H$, isto é, $g^{-1}Hg \subset K$ ou ainda, $H \subset gKg^{-1}$. Como K e gKg^{-1} possuem a mesma ordem, e como H e K são p -grupos de Sylow de G segue que eles possuem a mesma ordem, então H e gKg^{-1} possuem a mesma ordem, assim $H = gKg^{-1}$ e portanto H e K são conjugados.

□

Corolário 1. *Um grupo G possui um único p -subgrupo de Sylow H , se e somente se, H é normal em G .*

Por fim temos o último teorema de Sylow.

Teorema 7 (3º Teorema de Sylow). *Sejam p um primo e G é um grupo tal que $|G| = p^r m$, $p \nmid m$, e n_p o número de p -subgrupos de Sylow. Então,*

$$1. \ n_p \equiv 1 \pmod{p}.$$

$$2. \ n_p \mid m.$$

Demonstração. Seja $S := \{H \leq G \mid H \text{ é } p\text{-subgrupo de Sylow}\}$, logo $n_p = |S|$.

1. Pelo Teorema 5 temos $S \neq \emptyset$, logo fixando $P \in S$, considere a ação de $P \curvearrowright S$ dada por conjugação, ou seja,

$$\begin{aligned}\varphi_1 : P \times S &\rightarrow S \\ (g, Q) &\mapsto gQg^{-1}.\end{aligned}$$

Pelo Lema 2, temos

$$n_p \equiv |S^P| \pmod{p}. \quad (4)$$

Como $P \in S^P$, temos $|S^P| \geq 1$. Vamos mostrar que $|S^P| = 1$. De fato, suponha que exista outro ponto fixo $R \in S^P$. Então $pRp^{-1} = R$, para todo $p \in P$, logo $P < N(R)$ o normalizador de R . Como $P, R \in S$, temos que $|P| = |R| = p^r$.

Como $p^{r+1} \nmid |G|$ e $N(R) \leq G$, segue que $p^{r+1} \nmid |N(R)|$. Logo P e R também são p -subgrupos de Sylow de $N(R)$. Como $R \triangleleft N(R)$ pelo Corolário 1 temos $P = R$. Logo $|S^P| = 1$ e por (4) temos $n_p \equiv 1 \pmod{p}$.

2. Considere agora a ação de G em S por conjugação

$$\begin{aligned}\varphi_1 : G \times S &\rightarrow S \\ (g, Q) &\mapsto gQg^{-1}.\end{aligned}$$

Pelo Teorema 6, tal ação possui uma única órbita. Considere $\mathcal{O}(P)$ para algum $P \in S$, temos $n_p = |\mathcal{O}(P)|$. Pelo Teorema 2 temos

$$n_p = |\mathcal{O}(P)| = |G : \text{Stab}(P)|,$$

logo $n_p \mid |G| = p^r m$. Como pelo item 1 temos $n_p \equiv 1 \pmod{p}$ segue que $n_p \nmid p$ e portanto $n_p \mid m$.

□

Exercícios

1. O Teorema de Cayley sugere uma pergunta natural. Qual é essa pergunta?
2. Sejam G um grupo, X um conjunto e $G \curvearrowright X$ uma ação. Prove que $x \simeq_G y$ se, e somente se, existe $g \in G$, tal que $gx = y$ define em X uma relação de equivalência. Conclua que duas órbitas coincidem ou são disjuntas.
3. Prove que as aplicações definidas nos Exemplos 1-5 definem ações de grupos nos respectivos conjuntos.
4. Considere $G = O(n, \mathbb{R})$, $H = SO(n, \mathbb{R})$, a esfera $S^n := \{v \in \mathbb{R}^n; ||v|| = 1\}$ e as funções de $\phi_1 : G \times S^n \rightarrow S^n$ e $\phi_2 : G \times S^n \rightarrow S^n$ dadas pela multiplicação usual de matrizes. ϕ_2 é uma ação de H em S^n ? Descreva as órbitas de ϕ_1 , ϕ_2 , caso a segunda definir uma ação.
5. Seja $G \curvearrowright X$ uma ação. Prove que para todo $x \in X$ temos $\text{Stab}(x) \leq G$.
6. Sejam G um grupo e $H \leq G$. Considere o conjunto $N(H) := \{x \in G; x^{-1}Hx \subset H\}$. $N(H)$ é dito o **normalizador** de H em G . Prove que $N(H) \leq G$, e que $H \triangleleft N(H)$,
7. Seja G um grupo e p um número primo. Se $|G|$ é uma potência de p prove que $Z(G)$ é não trivial.
8. Seja G um grupo e p um número primo. Prove que se $|G| = p^2$ então G é abeliano. Encontre todos os possíveis grupos de ordem p^2 (*).
9. Encontre todos os subgrupos de Sylow de S_4 e de S_5 .
10. Sejam G um grupo finito, p e q números primos, e P e Q p, q subgrupos de Sylow de G , respectivamente, tais que $n_p = n_q = 1$, com $P \cap Q = \{e_G\}$, então $gh = hg$ para todo $g \in P$ e $h \in Q$.
11. Se G é um grupo tal que $|G| = 45$ então G é abeliano.

12. Se G é um grupo tal que $|G| = pq$ com $p > q$, primos, e p não divide $q - 1$. Então G é abeliano.
13. Seja $\varphi : G \rightarrow H$ um epimorfismo. Mostre que se P é um p -subgrupo de Sylow de G , então $\varphi(P)$ é um p -subgrupo de Sylow de H .